Towards a bifurcation theory for perturbed monomial dynamical systems modulo a prime

Marcus Nilsson

April 17, 2013

Abstract

We investigate perturbed monomial dynamical system over $\mathbb{F}_p$ given by iterations of $x \mapsto x^n + c \bmod p$, where $c \in \mathbb{F}_p$. Instead of study the systems one at a time we study all of them at the same time. The complex distibution of periodic points is visualized in the so called Periodic Point Diagram, which can be seen as a discrete version of the classical Bifurcation Diagram. We also prove some general results about the distribution of periodic points. We end the article with a conjecture about the total number of periodic points.

1 Introduction

We consider the dynamical system given by iterations of

$$h_c(x) = x^n + c \tag{1.1}$$

over the prime field $\mathbb{F}_p$, the set $\{0, 1, \ldots, p-1\}$ with addition and multiplication modulo p. We let $n \geq 2$ be an integer and $c \in \{0, 1, \ldots, p-1\}$. By h_c^r we mean the r-fold composition of h_c. The dynamics of $h_c(x)$ changes dramatically with the value of the parameter c. Classically we have a bifurcation if there is a sudden change in the dynamics at a certain parameter value, see for example [3]. If we use the classical definition of a bifurcation point we can say that we have a bifurcation for every value of c. When describing the dynamics we will concentrate on the number of periodic points. A point a is said to be a periodic point if $h_c^r(a) = a$ for some positive r, the smallest such r is called the period of a. We say that a is an r-periodic point. Since we are dealing with a finite set (all residues modulo a prime p) every point will after a number of iterations be mapped onto a periodic point. The set of points can therefore be partitioned into two sets, the periodic points and the preperiodic points that will eventually be mapped onto periodic points.

We will use the notation $\mathbb{F}_p^*$ for the multiplicative group of $\mathbb{F}_p$. We will visualize the dynamics of h_c on $\mathbb{F}_p$ by a directed graph $\mathrm{Graph}(V, E)$, where the the vertex set is $V = \mathbb{F}_p$ and the edge set E, is the set $\{(x, h_c(x)), x \in V\}$.

Example 1.1. Let us study the dynamics of the $h_c(x) = x^2 + c$ on $\mathbb{F}_7$ for all seven possible choices of c. We iterate the map $x \mapsto x^2 + c \bmod 7$. The result is shown in Figure 1.1. Here we can see that the dynamics changes a lot if we change the value of c.

The systems $x \mapsto x^2 + c$ on $\mathbb{F}_p$ have been studied before. In [8] Rogers discribes the connected components of the directed graph of $x \mapsto x^2$. Rogers stated that for $c \neq 0$ the dynamics seems to be beyond description. In [11] Vasiga and Shallit succeeded in describing the dynamics of $x \mapsto x^2 - 2$. Also Gilbert et al in [2] contributed to the understanding of the dynamics of $x \mapsto x^2 - 2$. We can see this already in Figure 1.1, the graphs for $c = 5$ and $c = 0$ seems more symmetric than the other graphs. In [4] the number of cycles (periodic orbits) of $x \mapsto x^n \bmod p$ are calculated by using Möbius inversion formula. Asymptotical behavior for the number of periodic points when $p \to \infty$ where investigated. The results from [4] where extended in [6] and in [7].

In this article we will construct a bifurcation diagram analogously to the classical diagram describing for example the bifurcations of the logistic map $x \mapsto rx(1 - x)$ over the real numbers. See for example [3] for details on this dynamical systems. In Figure 1.2 a bifurcation diagram for the logistic map is given. A variant of the Mathematica program suggested by [3] was used for producing the picture.

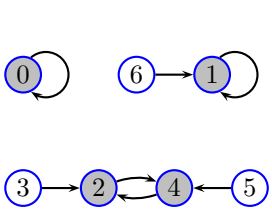
This article is organized as follows: In Section 2 we introduce the Periodic Point Diagram (PPD) and compare it with the classical bifurcation diagram. We also prove some general properties of the PPD. Then in Section 3 and Section 4 we investigate the properties of PPD in more detail for $n = 2$ and $n > 2$, respectively. In Section 5 we formulate a conjecture on the asymptotical behavior of the total number of periodic points of set $\{x \mapsto x^n + c; c \in \mathbb{F}_p\}$ of dynamical systems when $p \to \infty$.

2 The periodic point diagram

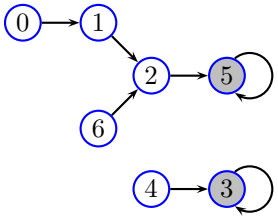
First of all there is an important difference between the bifurcation diagram we will construct for $x \mapsto x^n + c \bmod p$ and the classical one; our diagram is discrete. We will include every possible value of both x and c. We construct the diagram in the following way: On the horizontal axis we have all the possible values of c, $c \in \mathbb{F}_p$ and on the vertical axis we have the possible values of x, $x \in \mathbb{F}_p$. For each c we mark the x-values that are periodic points.

Example 2.1. Let us consider the dynamical system $x \mapsto x^2 + c \bmod 7$. In Figure 2.1 the bifurcation diagram for this system is shown. It is hard to see any pattern from one c to the next. However, there seems to be diagonal lines with no periodic points.

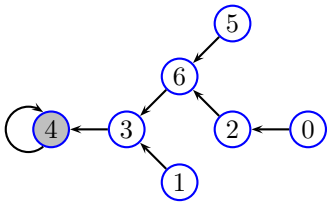
The diagram in Figure 2.1 was made by using a Mathematica program, that naively computes the periodic points for each c: Iterate every point in $\mathbb{F}_p$, p times then start saving the next p iterates. Then take the union of all resulting



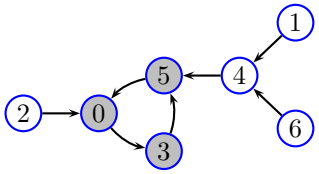
(a) $c = 0$



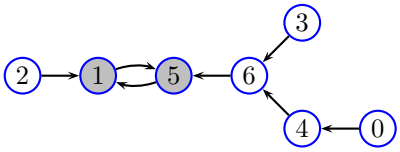
(b) $c = 1$



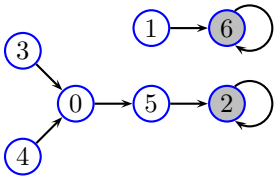
(c) $c = 2$



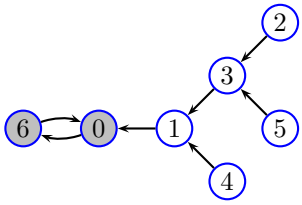
(d) $c = 3$



(e) $c = 4$



(f) $c = 5$



(g) $c = 6$

Figure 1.1: The dynamics of the seven systems $x \mapsto x^2 + c \bmod 7$.

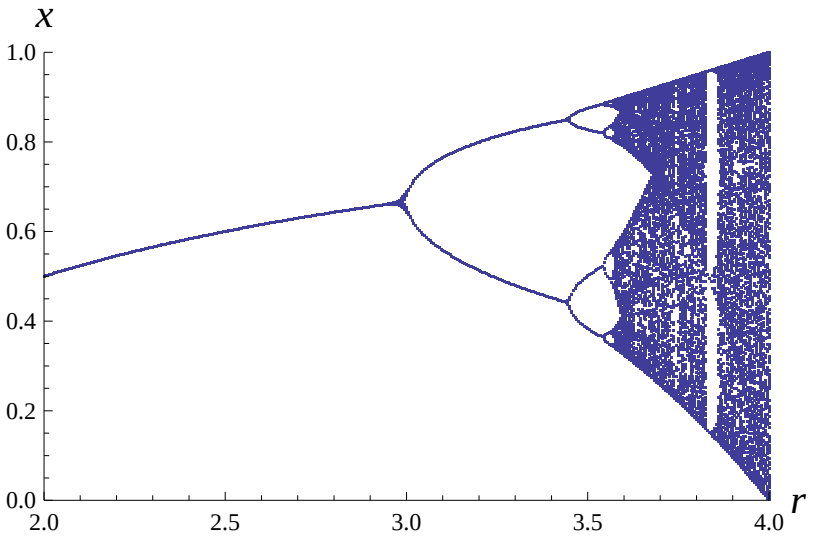


Figure 1.2: The bifurcation diagram of $x \mapsto rx(1-x)$ for $r \in [2,4]$. This is just iterations of the starting value $x = 0.5$.

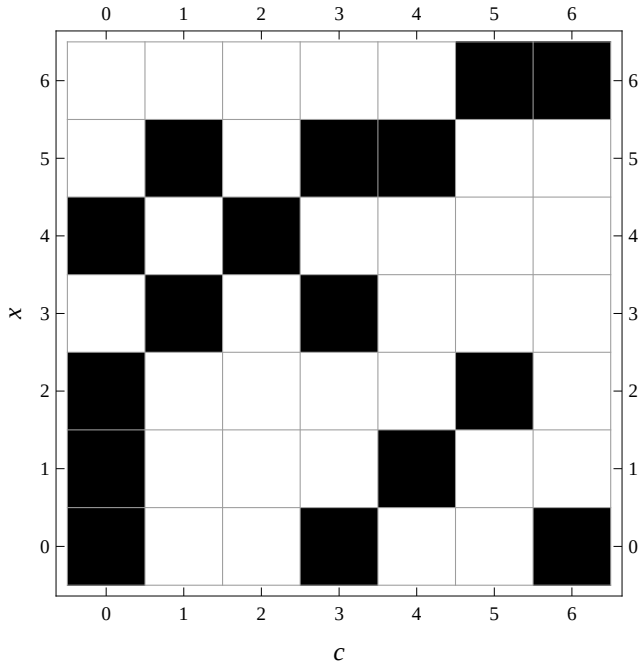


Figure 2.1: The bifurcation diagram of $x \mapsto x^2 + c \bmod 7$.

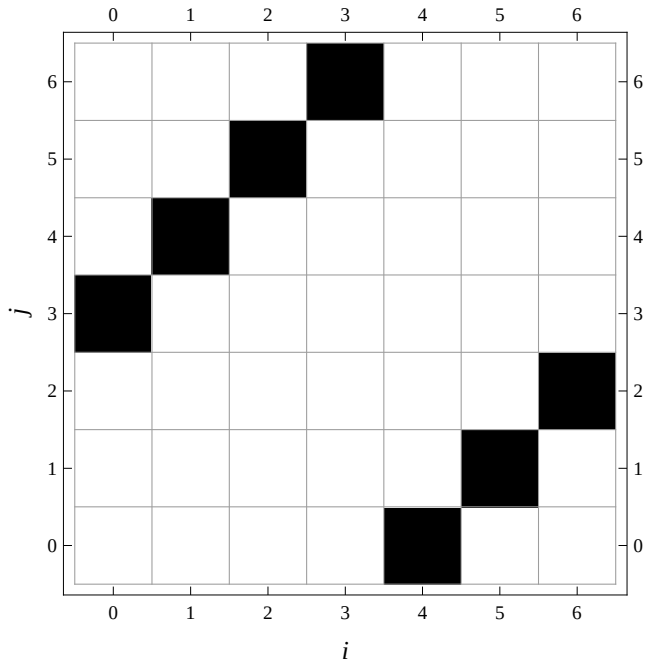


Figure 2.2: The diagonal line $j = i + 3 \bmod 7$ in the PPD$(h_c, 7)$.

points. In this way we are sure to have found all the periodic points and no preperiodic points. Of course there a more effective algorithms that uses for example Floyd's cycle finding algorithm (Tortoise and Hare), see [1, 5], but creating the diagrams in this article the naive way is enough.

We now make some formal definitions. First of all, instead of saying "bifurcation diagram" we call the diagram *Periodic point diagram* (PPD), it seems like a better name since we do not really have the same kind of bifurcation in our finite case as in the classical case. The PPD of the parametrized dynamical system given by iterations of the mapping $x \mapsto h_c(x)$ modulo p is denoted by PPD(h_c, p). Let $a \in \mathbb{F}_p$. By a diagonal line in the PPD(h_c, p) we mean all points (i, j) in the diagram satisfying the equation $j = i + a \bmod p$. For $a = 0$ we have the diagonal from the lower left corner to the upper right corner. All other diagonal lines are divided into two parts, see Figure 2.2.

Definition 2.2. By a *desert line* of PPD(h_c, p) we mean a diagonal line with no periodic points.

Example 2.3. Let us now consider the dynamical system $x \mapsto x^2 + c \bmod 71$. In Figure 2.3 we have its PPD. Here the desert lines are clearly visible.

Before we enter the discussion on how many desert lines there are, we take a look at some conditions for h_c to be bijective.

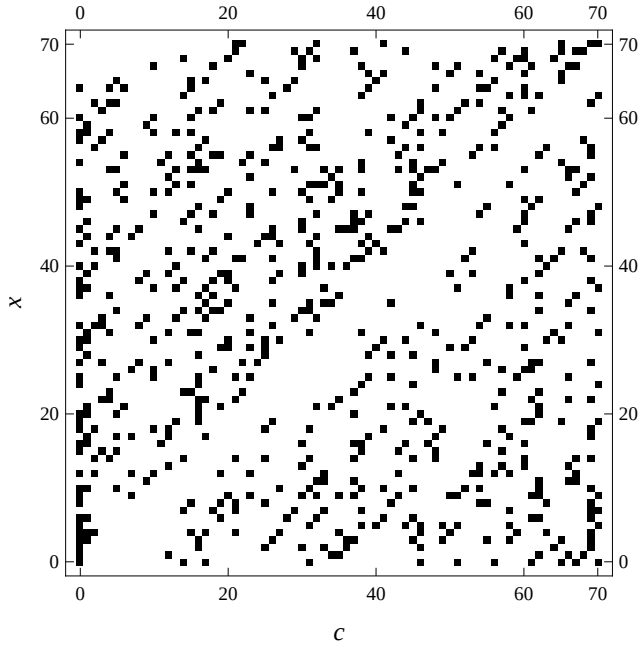


Figure 2.3: The bifurcation diagram of $x \mapsto x^2 + c \bmod 71$.

Lemma 2.4. *If h_0 is bijective then h_c is bijective for all $c \in \{0, 1, \ldots, p-1\}$.*

Proof. Assume that the map $h_0(x) = x^n$ is bijective. Let $x, y \in \mathbb{F}_p$. If $x^n + c = y^n + c$ then $x^n = y^n$ and this implies $x = y$ since $x \mapsto x^n \bmod p$ is bijective. □

In fact, we can generalize the lemma to: If h_c is bijective for one c it is bijective for all. Moreover, if the map h_c is bijective then the dynamical system can't have any preperiodic points. Hence the dynamics has a pure cycle structure if and only if h_c is bijective.

Theorem 2.5. *The dynamics of $h_c(x) = x^n + c$ has a pure cycle structure if and only if* $\gcd(n, p-1) = 1$.

Proof. In this proof we will use results from elementary number theory. See for example [9] for details on primitive roots and solutions of congruence equations. The theorem follows if we can prove that $x \mapsto x^n \bmod p$ is bijective if and only if $\gcd(n, p-1) = 1$. Let μ be a primitive root modulo p. Let $x, y \in \mathbb{F}_p^*$ then there are $i, j \in \{0, 1, \ldots, p-2\}$ such that $x = \mu^i$ and $y = \mu^j$. We have $x^n = y^n$ if and only if $ni \equiv nj \pmod{p-1}$. This equation has the unique solution $i \equiv j \pmod{p-1}$ (hence $i = j$ since they are both in $\{0, 1, \ldots, p-2\}$) if and only if $\gcd(n, p-1) = 1$. Also note that $x^n = 0$ in $\mathbb{F}_p$ if and only if $x = 0$. □

In the next section we will prove that there are exacly $(p-1)/2$ desert lines in $\mathrm{PPD}(x^2 + c, p)$ for $p \geq 3$.

3 The quadratic case

In this section we look at the PPD for the quadratic mapping $x \mapsto x^2 + c \bmod p$. We first recall the definition of quadratic residues and quadratic non-residues.

Definition 3.1. Let p be a prime and let a be an integer such that $\gcd(a, p) = 1$. We say that a is a *quadratic residue* if the equation $x^2 = a$ has a solution in $\mathbb{F}_p$. If it doesn't have a solution, then a is called a *quadratic non-residue*.

We have the following well known result for quadratic residues, see [9]:

Theorem 3.2. *Let p be an odd prime. Then there are $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic non-residues.*

Theorem 3.3. *Let $p \geq 3$ be a prime. If a is a quadratic non-residue modulo p then $j = i + a \bmod p$ is a desert line. If a is a quadratic residue there are two fixed points on the line $j = i + a \bmod p$. If $a = 0$ there are one fixed point on the line $j \equiv i \pmod p$. Hence, there are exactly $(p-1)/2$ desert lines in $\mathrm{PPD}(h_c, p)$.*

Proof. We have an r-periodic point at position (i, j) in the PPD-diagram if $h_i^r(j) = j \bmod p$. Consider the points (i, j) on the diagonal line $j = i + a \bmod p$. Assume that we have an r-periodic point on this line. That is, for some $j \in \{0, 1, \ldots, p-1\}$ we have

$$h_i^r(i + a) = i + a$$

We have

$$\left(h_i^{r-1}(i + a)\right)^2 + i = i + a,$$

and

$$\left(h_i^{r-1}(i + a)\right)^2 = a. \tag{3.1}$$

Hence, if a is a quadratic non-residue then (3.1) has no solution and $j = i + a \bmod p$ is a desert line. From Theorem 3.2 it follows that we have at least $(p-1)/2$ desert lines in the PPD.

Let $r = 1$ and let a be a quadratic residue. We have from (3.1) that $(i+a)^2 = a$. There are exactly two values of i that solves this equation since there are exactly two square roots of a quadratic residue. For $a = 0$ there is exacty one fixed point (for $i = 0$). So, we have exactly $(p-1)/2$ desert lines. □

4 The n-power case

In this section we will generalize our investigations from last section to the PPD of $x \mapsto x^n + c \bmod p$. First we note that if n and $p-1$ are relatively prime then it follows from Theorem 2.5 that we have a pure cycles structure for all values of c. This means that we have no desert lines in this case. Moreover, the whole PPD is filled, since every point is a periodic point. Before we learn more about the desert lines we recall some facts about n-power residues.

Definition 4.1. Let p be a prime and let $a \in \mathbb{F}_p^*$. Then a is said to be an n-power residue if $x^n = a$ has a solution in $\mathbb{F}_p$. Otherwise, a is called an n-power non-residue.

Theorem 4.2. *We have that $a \in \mathbb{F}_p$ is an n-power residue if and only if*

$$a^{(p-1)/\gcd(n,p-1)} = 1.$$

There are $(p-1)/\gcd(n,p-1)$ such a in $\mathbb{F}_p$. For each n-power residue a the equation $x^n = a$ has $\gcd(n,p-1)$ solutions in $\mathbb{F}_p$.

See for example [10] for a proof of this theorem and for more details on n-power residues.

Theorem 4.3. *We have that $j = i + a$ is a desert line in $\mathrm{PPD}(h_c, p)$ if and only if a is an n-power non-residues modulo p. Hence there are exactly $p - 1 - (p-1)/\gcd(n,p-1)$ desert lines. Moreover, if a is an n-power residue then there are $\gcd(p-1,n)$ fixed points on the line $j = i + a$. For $a = 0$ there is one fixed point (for $i = 0$).*

Proof. Consider the points (i, j) on the diagonal line $j = i + a$. Assume that we have an r-periodic point on this line. That is, for some $i \in \{0, 1, \ldots, p-1\}$ we have

$$h_i^r(i + a) = i + a.$$

We have

$$\left(h_i^{r-1}(i + a)\right)^n + i = i + a,$$

and

$$\left(h_i^{r-1}(i + a)\right)^n = a. \tag{4.1}$$

Hence, if a is an n-power non-residue then $j = i + a$ is a desert line.

If $r = 1$ and a is an n-power residue then from (4.1) we have $(i+a)^n + i = i + a \pmod p$ and hence $(i + a)^n = a$. From Theorem 4.2 it follows that there are $\gcd(n, p-1)$ different $i \in \mathbb{F}_p^*$ satisfying this equation. For $r = 1$ and $a = 0$ we have the unique solution $i = 0$. Hence there are exactly

$$p - 1 - \frac{p-1}{\gcd(n,p-1)} = \frac{p-1}{\gcd(n,p-1)}(\gcd(n,p-1) - 1)$$

desert lines in the PPD. □

Example 4.4. Let us look at the PPD of the dynamical system $x \mapsto x^5 + c \bmod 71$ in Figure 4.4. Here we see the increased number of desert lines compared to the $x \mapsto x^2 + c \bmod 71$ in Example 2.3.

We end this section with an observation regarding symmetry when n is odd.

Definition 4.5. By the *reduced Power Point Diagram* of $h_c(x)$ over $\mathbb{F}_p$ we mean the diagram we get by removing the column $c = 0$ and the row $x = 0$ from the PPD.

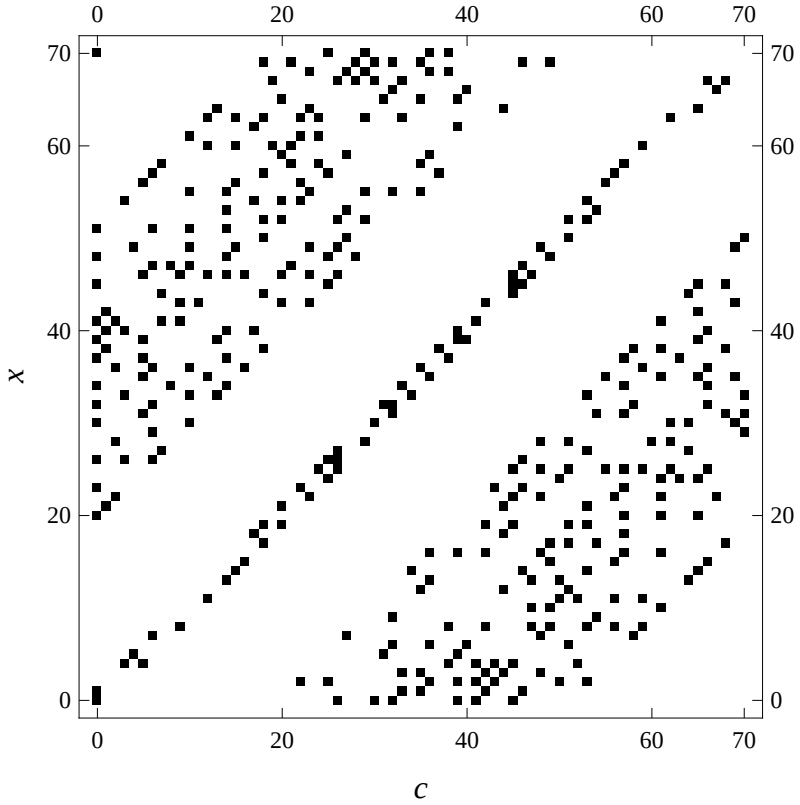


Figure 4.1: The PPD($x^5 + c, 71$).

Theorem 4.6. *If n is odd then the reduced* PPD *of h_c over $\mathbb{F}_p$ is symmetric with respect to the line $j = -i \bmod p$. That is, if a is an r-periodic point of $h_c(x)$ then $-a$ is an r-periodic points of $h_{-c}(x)$ ($-a$ and $-c$ are the additive inverses of a and c modulo p).*

Proof. We first observe that $h_{-c}(-a) = (-a)^n - c = -h_c(a)$ and that $h^r_{-c}(-a) = -h^r_c(a)$ for all $r \geq 1$. Assume now that a is an r-periodic point of $h_c(x)$. Then

$$h^r_{-c}(-a) = -h^r_c(a) = -a.$$

Moreover, $h^d_{-c}(-a) \neq -a$ for all $d < r$ since $h^d_c(a) \neq a$ for such d. Hence $-a$ is an r-periodic point of $h_{-c}(x)$. □

5 Conjectures about the number of periodic points

From Theorem 4.3 it follows that there are exactly p fixed points in total to the set $\{h_c(x) : c \in \mathbb{F}_p\}$ of perturbed monomial systems modulo p. Hence, among the marked points in the PPD there are exactly p that are fixed points.

In this section we will consider the problem of computing the number of periodic points for all values of c, that is the number of marked points in the PPD. Let $\mathrm{Per}(h_c, p)$ be the number of periodic points of the class of dynamical systems $x \mapsto h_c(x) \bmod p$ (the number of marked points in the $\mathrm{PPD}(h_c, p)$). The only case when it is easy to compute $\mathrm{Per}(h_c, p)$ is when $\gcd(n, p-1) = 1$. Then we have $\mathrm{Per}(h_c, p) = p^2$. From 4.3 we have the following rough estimate

$$p \leq \mathrm{Per}(h_c, p) \leq \frac{p(p-1)}{\gcd(n, p-1)}. \tag{5.1}$$

We have used the fact that there can be at most p periodic points on each non-desert line.

We will use a Mathematica program for computing the number of periodic points. The program is based on Floyd's cycle finding algorithm [1, 5]. The naive program described in Section 2 for producing the PPD:s is too slow for large primes. Let us look at some examples.

Example 5.1. Let us calculate the number of periodic points of $h_c(x) = x^2 + c \pmod p$ for the first 1000 primes. The result is shown in Figure 5.1.

Example 5.2. Consider the dynamical system $h_c(x) = x^{12} + c$. In Figure 5.2 $\mathrm{Per}(x^{12} + c, p)$ is plotted for the first 1000 primes. Here we see that the diagram seems to contain four different curves. These are branches corresponding to the four possible different values of $\gcd(12, p-1)$ for odd primes p. The possible values are 2, 4, 6 and 12. The lowest branch corresponds to 12 and the highest to 2.

We call the kind of diagrams shown in the examples *Total Periodic Diagrams* (TPD). The Total Periodic Diagram for $h_c(x) = x^n + c$ for the first m primes is denoted by $\mathrm{TPD}(h_c, m)$.

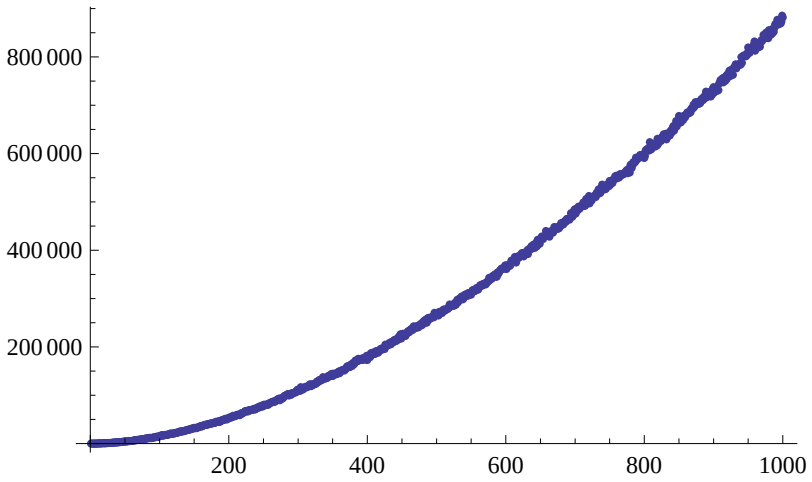


Figure 5.1: $\mathrm{Per}(x^2 + c, p)$ for the first 1000 primes. Note that the value of the horizontal axis is the ordinal of the prime number.

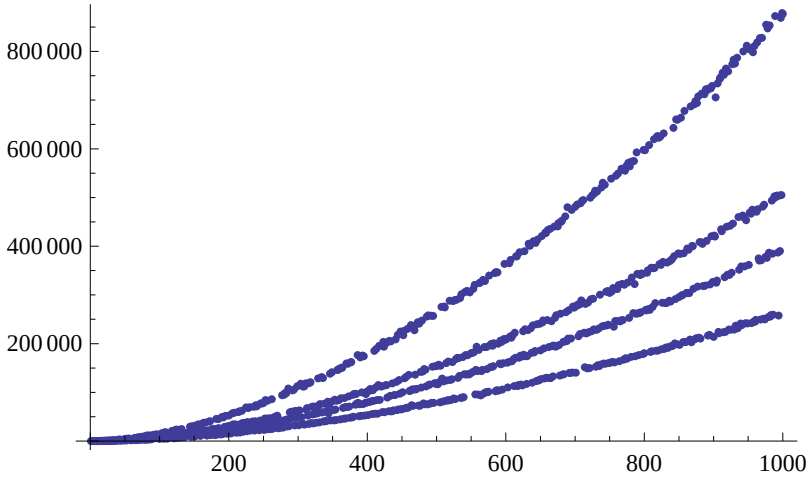


Figure 5.2: $\mathrm{Per}(x^{12} + c, p)$ for the first 1000 primes.

Conjecture 5.3. *Let $n \geq 2$ be an integer. Let $h_c(x) = x^n + c \bmod p$. The* $\mathrm{TPD}(h_c, m)$ *then contains as many branches as there are possible values of* $\gcd(n, p-1)$.

It would of course also be interesting to find a simple asymptotic estimate for $\mathrm{Per}(x^n + c, p)$ when $p \to \infty$. Thus, we are interested in finding a function $f_d(p)$ such that

$$\lim_{\substack{p\to\infty \\ \gcd(n,p-1)=d}} \frac{\mathrm{Per}(x^n + c, p)}{f_d(p)} = 1, \tag{5.2}$$

for a possible value d of $\gcd(n, p-1)$.

6 Discussion

Some of the results of this article can be generalized to arbitrary functions $f(x)$ defined on $\mathbb{F}_p$. Desert lines will occur also in the general case. There will be as many desert lines as there are $a \in \mathbb{F}_p$ such that $f(x) = a$ has no solutions in $\mathbb{F}_p$. It is also possible to extend some of the results to more general structures than the fields $\mathbb{F}_p$, for example the rings of integers modulo an composite integer.

References

[1] R.W. Floyd. Non-deterministic algorithms. *J. ACM*, 14(4):636–644, 1967.

[2] Ch. L. Gilbert, J. D. Kolesar, C. A. Reiter, and J. D. Storey. Function digraphs of quadratic maps modulo p. *Fibonacci Quart.*, 39:32–49, 2001.

[3] Richard A. Holmgren. *A first course in discrete dynamical systems.* Springer-Verlag, 1996.

[4] A. Yu. Khrennikov and M. Nilsson. On the number of cycles of p-adic dynamical systems. *Journal of Number Theory*, 90(2):255–264, 2001.

[5] Donald E. Knuth. *The Art of Computer Programming, vol. II: Seminumerical Algorithms.* Addison-Wesley, 1969.

[6] M. Nilsson. Fuzzy cycles of p-adic monomial dynamical systems. *Far East J. Dynamical Systems*, 5(2):149–173, 2003.

[7] M. Nilsson. Computational aspects of monomial dynamical systems. *The computer journal*, 2007. Advanced Access, doi:10.1093/comjnl/bxm100.

[8] T. D. Rogers. The graph of the square mapping on the prime fields. *Discrete Mathematics*, 148:317–324, 1996.

[9] Kenneth .H. Rosen. *Elementary number theory and its applications.* Pearson, 2010.

[10] W. Sierpinski. *Elementary Number theory*. North-Holland, 1988.

[11] T. Vasiga and J.Shallit. On the iteration of certain quadratic maps over gf(p). *Discrete Mathematics*, 277:219–240, 2004.